咳血的独角兽丨互联网的幕后攻防

原创：半佛仙人 半佛仙人 昨天

1.

风险控制，“知道”的人多，“了解”的人少。

我想谈谈一些真实发生的案例，来给大家展示一下风险控制这个职业，能为公司产生什么样的价值或者损失。

这些内容我保证是你花钱都买不到的。但可以从中领悟多少进攻或者防守的思路，就全看自己的悟性了。

老朋友们应该都知道，我本职工作是做风控的，从线下尽调，信用卡，金融，电商，安全，数据，基本每一个领域的风险管理，我都玩过，并且玩的不错。

风险控制，或者说风险管理，在互联网公司中，一直是一个比较尴尬又不上不下的岗位。

说风控不重要吧，你去问任何一个公司的老板，都可以balabala说出各种风控的重要性，大道理讲到你吐血。

说风控重要吧，在绝大多数公司的实际情况中，风控都是为业务方让路的，运营部门要增长，市场部门要投放，活动部门要大促，这些都有明确的指标考核，而这些部门由于直接影响公司数据，进而影响公司讲故事融资，所以往往特别强势，风控这种做减法的部门，在他们眼中更是业绩的阻碍，最好统统赶走。

多数老板为了面子好看，对外大力吹风控；为了里子好看，对内往往是默许业务部门Diss风控甚至搞点小动作的，所以到最后，风控往往里外不是人。

某位老板曾经在酒后对我说过，你们这些风控，如果业务没有出现风险，养你们就像养猪；如果业务出了风险，养你们还不如养猪。

某种程度上，这话是对的，风控只是业务的辅助。

但在另一些维度中，业务营销如果风控放水，那么多少钱都只能打水漂。

以下我讲谈及一些案例，以及其中的诀窍，功防技巧。

本文中我所介绍的进攻手段我自己是知道怎么防守甚至怎么反杀的，这也是我的专业价值所在

集中注意，我们开始案例讲解。

2.

某某咖啡，号称打倒星巴克，教育中国人的咖啡习惯，不差钱，估值数十亿美金，即将尝试美股IPO，一年亏损几个亿都不当回事的公司，在今天把自己的一堆咖啡机做了抵押，换取了4500万人民币抵押贷款，这很喜感。

当然他们对外解释是轻资产运营，设备利用最大化，这话是不是真的，每个人都有自己不同的见解。

但作为2018年烧钱最猛，同样也是增长最猛的品牌之一，营销方面我不好说，只能说他们的风控做的不够到位，当然也可能是为了漂亮的数据搞投资，默许风控滚开。

某某咖啡曾有一个非常经典的用户拉新活动，就是只要你邀请人别人注册并下单，你就可以获得一张免费喝咖啡的券，由于新注册用户有默认的免费券，所以等于是存在无成本套咖啡券的漏洞。

A邀请B注册并下单。

A获得一张免费券，B免费下单。

所以，只要有批量注册的手机号，就可以大量开始刷咖啡券了，只需要不停地用新手机号注册，然后下单，然后就有券，操作一次可以免费喝至少2杯咖啡，美滋滋。

而市场上买一次手机号带验证码注册的成本，是2毛到1元。

如果你能批量使用2毛一次的成本，换取2杯免费咖啡，那么你完全可以第一杯自己喝，第二杯以极低的价格卖给身边的同事，这种便宜很少有人会拒绝。

而且这个已经产业化了，标准灰产。

在某些二手交易平台上，直接搜索，就有各种代下单。

除了免费咖啡（他们被薅实在太狠了）之外，更多的是一些打折券，尤其是有一段时间，XX疯狂在发3折券和2.8折券，这些券的领取方式更简单，只要在H5页面输入手机号，就可以领取。

所以在刷号注册拿免费券之后，那些不能再享受新人券的账号，可以再拿来领一些折扣券，同样可以获取套利。

保守估算，其相关营销投入的接近一半，是被刷掉了，没有获取到真实有效的用户，这可是亿级别的损失。

并且这种手动机器注册，并且用完首单资格再领券的玩法，适合一切有分享领券功能的电商和外卖平台。

当然，无限制的下单也不可能，公司也不是傻子，总有一些规则可以拦截掉异常订单，只不过他们的风控一肚子本领无从下手而已。

你拦截了订单，就是拦截了GMV，你拦截了GMV，就是拦截了业务的KPI，你拦截了业务的KPI，就拦截了公司融资，对于很多toSBVC的公司而言，这比杀了他们还难受。

所以很吊诡的是，风控仇视羊毛党，营销仇视风控，同时营销又跪舔羊毛党。

毕竟KPI和年终奖是自己的，亏损是公司的，岂不美哉？

3.

说到最近风投正劲的几家O2O公司，就是各类XX买菜，XXX鲜，XX社区之流。

他们一直在烧钱，且优惠多多风控不多。

感谢他们的努力，很多羊毛党已经很久没有花钱买菜了，厉害一点的羊毛投资，各种拉新账户的余额加起来有6位数甚至7位数，基本只要公司不倒，买东西就不用花钱。

车厘子大闸蟹精酿啤酒进口牛排海鲜之类的消费升级，早就给他们吃腻了。

先说XX买菜，他们最近烧钱最厉害。

其拉新活动是，新人注册有2张大额券，满XX元，减XX元，里面的东西最划算的是牛奶，扣除优惠券金额后，存在很大的套利空间。

但是这家公司多少还有点风控意识的，其拉新套利单纯使用接码平台注册是没有意义的，因为会校验支付账户信息以及下单频次，同一个支付账户多次使用不同账号，或者同一台设备多次使用不同账号等等，会被直接拦截。

所以很多专业刷子，会使用专业设备和专业账户来绕过规则，他们的风控漏洞对于专业选手而言非常明显，只需要一点简单的伪装，这些基于用户信息的核身规则都会失效。

再说XXX鲜，在圈内被称为羊毛X鲜，推广及其豪爽，漏洞多不胜数。

首先是拉新，现在的拉新是只有推荐下单后各享受大额满减的，而早期的时候，还有满多少人送多少余额的活动。

利用某些平台，及广义地址（就是收货地址只留小区，不留具体门牌号，靠配送员电话口述），连伪装支付账户都不需要（他们没有做校验），就可以开刷，并且上面的某些硬通货很便宜，特别适合套利，别忘了，还有送余额的活动，这些余额就是纯赚的，可以买一切高折现率的产品，非常划算。

其风控之简陋，简直是羊毛党的提款机。

不仅没有收货人一致性校验，没有支付账号限制，没有LBS规则，没有用户血缘关联，没有实时热点监控，没有虚拟号段封锁，连IP墙和设备号限制都没有，可以一台手机，一个支付账户外加一个接码平台，就能无尽的刷。

可能是被刷太厉害了，导致现在不搞余额活动了，只给大额券，盈利少了不少，不过首单大额券，依然还是有吸引力。

所以你们看，如果风控不到位，这些公司的营销费用，全都白给。

随着黑产技术的进步，风控不好的公司，已经没法靠烧钱赢市场了。

4.

连说了2个套取新人优惠以及券的案例，我们讲点别的。

大家都知道苹果手机吧？这是一种硬通货，手机市场唯一的硬通货。

而很多新兴的社交电商平台，都是拿苹果手机，当做引流商品的。

什么叫引流商品？就是这个产品本身赔钱，但是吸引你来我店里消费，成为我的会员，你可能不止买这一个产品，我可以在别的商品上赚到钱。

就像很多饭店的特价菜一样，靠特价菜吸引你进店消费。

他们的苹果手机，出售价格往往是低于进货价的，而且补贴力度不小，起码我就知道某平台的XSMax，经常性低于市价300到500，这就存在了套利空间。

要知道黄牛正常倒卖苹果手机，一台往往也就100到200的利润，而如果能批量搞到这些引流款的手机，其利润非常可观。

所以各路黄牛都在试图获取更多特价菜。

由于这里面的利润很吸引人，这些平台对于引流款的看管都是很严的，普通的进攻手段是没有办法绕过风控规则的。

但是聪明的黄牛，都是用肉鸡操作。

什么是肉鸡？

就是这人不是虚拟的机器，而是真正的人，是一个活生生的用户。

大家都知道人肉刷单吧，就是平时该买啥买啥，偶尔有黄牛联系的时候，就帮下单刷一下商品，搜索，点击，聊天，砍价，支付，一条龙，就是活生生的人，只不过10单正常交易里有2到3单刷单而已。

目前苹果代下单的肉鸡价格是50元一单，很多人业余做肉鸡兼职，给自己加加鸡腿。

据我了解到的现状是，很多平台的引流款苹果手机，起码70%是被肉鸡刷走了，肉鸡刷走后手机流到了市场上，所以我们才总能买到各种低于市价的便宜正品手机，大家各取所需，也很好。

5.

来个高阶点的，锁价套利。

上面提到了苹果手机。

由于国内的电子市场非常发达，而苹果手机的需求又非常旺盛，所以往往苹果手机的价格是一天2变，可能一台手机早上是7000元，中午是7100元，下午是6900元，第二天是6850元。

大宗商品，价格频繁波动，某种程度上，苹果手机可以算作一种期货。

那么既然是期货，就存在空手套白狼的纯套利空间。

一般来说，电商平台是不太会给你这个空间的，你买便宜是你运气好，你买贵了就是买贵了，不管你是黄牛还是肉鸡还是正常客户，不管价格是便宜还是贵，你都应该是在某个固定时间以某个固定价格来买到这个商品。

但是尽管电商规则是这么设置的，但是可以从支付环节入手锁定价格。

例如某些电商平台曾经出现过漏洞，就是如果付款时，价格为A，选择某付款通道，选择支付方式为借记卡，卡中余额不足，就会支付失败，但是这笔支付订单可以保留好几天，在这个过程中可以随时以A价格完成支付，进入发货。

所以很多黄牛就会下单，然后故意支付失败，等着看平台调价，如果涨价了，价格高于A不少，他们就付A的钱拿货，发货地直接填付给他们钱的买家，空手套白狼；如果价格低于A，就取消订单，不要了。

再举个利用余额不足锁定价格的案例。

某著名连锁披萨餐厅，出现过一种漏洞，就是购买某个数百元的套餐，在付款时如果卡种余额是特定的XX元，再配合某个批次是优惠券，则可以触发几十块买到几百块的套餐，一家人只花几十块就成吃到不想再吃，很有趣。

同理，某连锁商超的电子会员系统，同样出现了支付余额的漏洞，可以低价搞到大额优惠券和卡，这种机会往往稍纵即逝。

国内有专门的黑产团队，每天都在利用支付失败这一条件来试探漏洞，因为支付是独立的体系，电商是电商的体系，只要是不同体系的交互，就一定存在套利空间。

这是不可避免的。

6.

换一种玩法。

大家知道套现吧？

就是把信用卡的额度，变成现金，这笔现金可以拿去投资，周转。

如果直接用信用卡取现的话，是要收取高昂的提现费用，并且被取出的额度按日计息，无法享受到信用卡的免息期。

所以如何各种渠道，把信用卡的额度变为无利息的现金，是一门生意。

当前最流行的就是各种二维码和各种Pos机，本质原理就是虚构一款商品，用信用卡刷这款商品，在银行眼中是正常消费，额度享受免息，但实际情况是刷卡人获得了现金。

这么操作，也是有成本的，成本在0.38%到1.2%之间。

所以如果有更低成本的套现渠道，就可以无风险套利。

某些疏于做支付风控的互联网公司，就有这样的漏洞。

大家还记得空空狐么，一家做二手交易，巅峰时到达过市场份额第三（第一第二是闲鱼和58），后来创始人和投资人决裂，疯狂撕逼。

很多人当时评价老板不成熟，投资人不靠谱，行业门槛高云云，实际都搞错了。

空空狐是被套现套死的。

当时为了增加市场占有，空空狐想出了这样一个营销方案，就是用信用卡支付，空空狐补贴手续费，他们没有意识到支付风险，也没有专业风控对交易补贴做风险兜底策略。

这种操作一放开，这家公司就已经死了。

由于空空狐是二手交易平台，所以买卖双方都可以自由上架货物并交易，在这个过程中还补贴信用卡手续费，那就等于是可以自由套现。

空空狐市场份额第三的GMV，就是这么来的，全都是虚假交易和套现，他们老板还开心的认为自己要成了，等到他们意识过来情况不对的时候，已经无钱可烧了。

空空狐成为了历史的尘埃。

因为套现存在大量的无风险获利，所以专门会有一支黑产团队做套现生意，他们会用爬虫爬取各家公司的营销政策，然后找出那些补贴交易的漏洞，再把资金放到上面去滚动获利，收益丰厚。

信用卡，某呗，某白条，某某付，只要是可以用于分期的产品，都可以用来做套现交易，规模最大的还是信用卡。

银行信用卡规模发卡规模和交易金额的不断攀升，表象是人民消费水平提高，而表象后面的本质，这些交易里，究竟有多少是被套走了呢？里面损失了多少利息收益和资金成本呢？

答案是百亿级别。

7.

共享单车，很多人都知道吧？

共享单车的押金，很多人都咬牙切齿吧？

如果我告诉你，共享单车的押金，也存在被黑产搞走的风险，好几家倒掉的共享单车公司，死因是押金被黑，你是不是不知道该说什么？

押金可以存，可以取，并且基本都是走支付机构接口的，很多公司的单车押金都是作为一个池子存在一起的。

当你提取押金的时候，会选择一个支付机构账号收款，资金池会和支付账号发生一次交互，这里面需要做相关的传输风控，需要定位打款的账号，定位信息，定位token，定位身份，做到多信息符合逻辑勾稽，才能打款。

而有些风控不严（共享单车没啥风控）的公司，在固定的发版日，会出现短时间的提现异常。

这个异常不是说不给你钱，而是可以利用机器伪装，伪装成不同的支付账号，多收钱。

某些共享单车，收了199押金，最后提现环节被人黑，掏了几十个199出去。

当然，这种极其内部的漏洞（短短十几分钟的系统真空），外界很难直接探知，是谁泄露了发版时间？是谁泄露了调用规则？

再联想一下最近某快完蛋的单车公司严查腐败，你猜猜内外勾结赚了多少？

当然说到内外勾结，最骚的还是某互金公司。

其某总监把公司内部的各种规则漏洞透露给某个媒体，然后对方写了一篇深度黑稿，各个黑到精髓上，然后公司大惊失色，大力投资在风控和PR上，作为控制投放资源和采购的总监，捞了好大一笔。

这种内鬼，最为致命，很多坚固的堡垒，都是从内部被攻破的。

8.

你知道看新闻，看视频，下载APP可以领奖金的那些应用么？

就是某某条这种，阅读多久多久，拉新多少多少，直接给现金。

你知道挂机软件吗？

就是游戏挂机常见的那种软件。

这种软件的原理就是通过脚本控制手机操作，然后模拟人的行为，解放人的双手。

那么问题来了，既然可以挂游戏，为什么不能挂一些送钱的APP呢？二手网站上有很多人公开售卖这种工具。

很多被低价回收的二手安卓手机，没有再次售卖的价值，被拿去干什么了呢？

嘿嘿嘿。

既然旧手机用不到了，何不挂上这些，去薅点钱呢？

虽然赚的不多，但收益稳定，操作可控，多好的事情。

你猜猜这些APP的巨额流量背后，有多少是僵尸呢？

又或者说，这些僵尸，是不是公司自己的培育的呢？这样连补贴都不用给，但可以计入营销费用，你想，这些差价哪去了？

9.

洋洋洒洒讲了这么多案例，相信各位读者已经感受到了风险控制这个岗位的重要性，风控做不好，运营和市场投放永远是拿钱打水漂。

而比起和羊毛党的战斗，风控最大的问题永远来自背后，来自虎视眈眈的业务方和想着拿内部数据获利的腐败团伙，这是我多年战斗下来最深的感触。

除了业务成本，用户数据的安全风控，则更为重要。

业务投放只是钱的事情，而用户隐私，是法律的事情。

很多掌握大量用户信息的互联网公司，其风险意识之淡薄，难以置信。

以前做进攻测试的时候，发现国内大批互联网公司的数据库没有做到内外网分离，甚至很多密码都是默认的admin和guest，还有123456，若是碰上别有用心且不惧法律的黑客，可以轻松把数据搞出来然后丢到黑市上打包卖掉。

是不是骚扰推销电话特别多？是不是营销短信越来越密集了？是不是各种奇怪的推送都来了？

他们从哪里获得的数据呢？

就从各个风控意识淡薄的公司里获取的。

天网年代的个人隐私，确实是很奢侈的事情。

唯一值得欣慰的是，在隐私暴露面前，我们是人人平等的，不会因为你的金钱地位高低而有所变化。

这可能是除了死亡之外，为数不多人人平等的事情。

但我一点都不开心。

你们呢？

公众号：半佛仙人（ID：banfoSB）
微博：半佛仙人正在装
知乎：半佛仙人
这是一个神奇的男人，你完全猜不出他会写出什么，他自己也不知道。

长按下图二维码关注，你将感受到一个朋克的灵魂，**且每篇文章都有抽奖，抽到你害怕。**

感谢你的阅读，下面是1个抽奖链接按钮，4月6日晚上19点开奖，一共1888元，666个红包，接到了广告，感谢大家支持。

如果你转发了本篇文章（分享朋友圈概率加倍）或者点击了【在看】，则中奖概率会提升，感谢支持！

【转发（朋友圈翻倍）】或者【在看】后，中奖概率会提升~点我抽奖，点我抽奖！